

## Issues

#	Project	Tracker	Status	Subject	Assignee	Updated
9758	Ruby trunk	Feature	Open	Allow setting SSLContext#extra_chain_cert in Net::HTTP	openssl	03/18/2019 10:12 PM
8720	Ruby trunk	Bug	Open	ECB mode seems to be broken	openssl	09/13/2015 03:30 AM
5103	Ruby trunk	Feature	Feedback	[ext/openssl] Object equality for objects based on ASN.1 structures	openssl	09/13/2015 03:32 AM
5102	Ruby trunk	Feature	Feedback	[ext/openssl] Purpose of OpenSSL::PKCS12.new / Allow changing the password	openssl	09/13/2015 03:33 AM
7400	Ruby trunk	Feature	Assigned	Incorporate OpenSSL tests from JRuby.	openssl	09/13/2015 03:08 AM
8178	Ruby trunk	Bug	Assigned	OpenSSL::PKCS7::SignerInfo	openssl	09/13/2015 03:13 AM
13100	Ruby trunk	Bug	Assigned	OpenSSL::PKey::EC#public_key_group	openssl	01/08/2017 05:51 AM
6493	Ruby trunk	Bug	Feedback	OpenSSL::SSL ignores DN if subjectAltName is specified	openssl	09/13/2015 03:32 AM
9833	Ruby trunk	Bug	Open	OpenSSL::X509::Certificate#inspect	openssl	09/13/2015 03:26 AM
10098	Ruby trunk	Feature	Assigned	[PATCH] Timing-safe string comparison for OpenSSL::HMAC	openssl	02/07/2019 07:40 AM
6047	Ruby trunk	Feature	Assigned	read_all: Grow buffer exponentially in generic case	openssl	09/13/2015 03:19 AM
8219	Ruby trunk	Bug	Assigned	ruby 2.0.0-p0 socket.recv MSG_OOB problem?	openssl	09/13/2015 03:11 AM
9822	Ruby trunk	Bug	Assigned	Ruby doesn't respect system OpenSSL configuration	openssl	02/06/2018 03:41 AM
6256	Ruby trunk	Feature	Feedback	Slightly improve ruby_qsort performance	MartinBosslet (Martin Bosslet)	01/10/2019 01:51 PM
15268	Ruby trunk	Bug	Open	Solaris test/drb/test_drbsl.rb	openssl	11/06/2018 03:48 PM
6133	Ruby trunk	Feature	Assigned	SSLSocket#shutdown	openssl	09/13/2015 03:22 AM
9830	Ruby trunk	Feature	Assigned	Support for GOST private/public keys	openssl	09/13/2015 03:10 AM
10519	Ruby trunk	Feature	Open	TLS Renegotiation	openssl	09/13/2015 03:29 AM
9613	Ruby trunk	Feature	Open	Warn about unsafe openssl ciphers	openssl	09/13/2015 03:27 AM
9504	Ruby trunk	Bug	Assigned	X509 certificate incorrectly loaded (because of try-pem-first-else-asn1)	openssl	09/13/2015 03:10 AM